An abundance of invariant polynomials satisfying the Riemann hypothesis

Koji Chinen[*]

29/4/2007

Abstract

In 1999, Iwan Duursma defined the zeta function for a linear code as a generating function of its Hamming weight enumerator. It can also be defined for other homogeneous polynomials not corresponding to existing codes. If the homogeneous polynomial is invariant under the MacWilliams transform, then its zeta function satisfies a functional equation and we can formulate an analogue of the Riemann hypothesis. As far as existing codes are concerned, the Riemann hypothesis is believed to be closely related to the extremal property.

In this article, we show there are abundant polynomials invariant by the MacWilliams transform which satisfy the Riemann hypothesis. The proof is carried out by explicit construction of such polynomials. To prove the Riemann hypothesis for a certain class of invariant polynomials, we establish an analogue of the Eneström-Kakeya theorem.

Key Words: Zeta function for codes; Riemann hypothesis; Perfect code; Eneström-Kakeya theorem; reciprocal equation; Invariant polynomial ring.
Mathematics Subject Classification: Primary 11T71; Secondary 94B05, 30C15.

1 Introduction

Let p be a prime, $q = p^r$ for some positive integer r and we denote the finite field with q elements by $\mathbf{F}_q$. Let C be an $[n, k, d]$-code over $\mathbf{F}_q$ with the Hamming weight enumerator $W_C(x, y)$. Duursma [4] defined the zeta function for C as a generating function of $W_C(x, y)$. Then the author [2] considered the case of so-called "formal weight enumerators", noticing that Duursma's definition can be extended for other homogeneous polynomials than the weight enumerators of actual codes. Taking these into account, we start from the following definition:

Definition 1.1 *For any $q \in \mathbf{N}$ ($q \geq 2$) and any homogeneous polynomial of the form*

$$W(x, y) = x^n + \sum_{i=d}^{n} A_i x^{n-i} y^i \quad (A_i \in \mathbf{C},\ A_d \neq 0) \tag{1.1}$$

[*] Department of Mathematics, School of Science and Engineering, Kinki University. 3-4-1, Kowakae, Higashi-Osaka, 577-8502 Japan. E-mail: chinen@math.kindai.ac.jp

there exists a unique polynomial $P(T) \in \mathbf{C}[T]$ of degree at most $n-d$ such that

$$\frac{P(T)}{(1-T)(1-qT)}(y(1-T)+xT)^n = \cdots + \frac{W(x,y)-x^n}{q-1}T^{n-d} + \cdots. \qquad (1.2)$$

We call $P(T)$ and $Z(T) = P(T)/(1-T)(1-qT)$ the zeta polynomial and the zeta function of $W(x,y)$, respectively.

For the proof of existence and uniqueness of $P(T)$, see Appendix. If $W(x,y) = W_C(x,y)$ for some linear code C, then we take q in the above definition as $\sharp\mathbf{F}_q$, but if $W(x,y)$ is not related to an existing code, then q must be chosen suitably according to what meaning $W(x,y)$ has.

In the case $W(x,y) = W_C(x,y)$, the zeta polynomial $P(T)$ for $W_C(x,y)$ is of particular interest when C is self-dual, because it has the functional equation

$$P(T) = P\Big(\frac{1}{qT}\Big)q^gT^{2g} \qquad (1.3)$$

($g = n/2+1-d$, see [5, p.59]), which is a result of the fact that $W_C(x,y)$ is invariant by the MacWilliams transform

$$\sigma_q := \frac{1}{\sqrt{q}}\begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix}, \qquad (1.4)$$

where we define $f^\sigma(x,y) = f(ax+by, cx+dy)$ for $f(x,y) \in \mathbf{C}[x,y]$ and a linear transformation $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

The functional equation (1.3) is the same as that of zeta functions of algebraic curves, so we can formulate the Riemann hypothesis (see Duursma [6, Definition 4.1]). Even if $W(x,y)$ does not correspond to an actual code, we can formulate the Riemann hypothesis in the same way provided that $W^{\sigma_q}(x,y) = W(x,y)$ because it is this invariance that yields (1.3):

Definition 1.2 *The code C (or the invariant polynomial $W(x,y)$) satisfies the Riemann hypothesis if all the zeros of $P(T)$ have the same absolute value $1/\sqrt{q}$.*

Duursma deduces various interesting properties of $P(T)$ and discusses their possible applications to the coding theory (see [5, 6, 7]).

Finding an equivalent condition for the Riemann hypothesis above seems still an open problem, but Duursma asks the following ([6, Open Problem 4.2]):

Problem 1.3 *Prove or disprove that all extremal weight enumerators satisfy the Riemann hypothesis.*

A self-dual code C is called extremal if it has the largest possible minimum distance (see Pless [11, p.139]). There are 4 well-known sequences of extremal self-dual codes (Types I, II, III and IV, see Conway-Sloane [3]). The extremal code is also characterized by its weight enumerator $W_C(x,y)$: the code C is extremal if d of $W_C(x,y)$ in (1.1) is the largest among all the self-dual weight enumerators of degree n over $\mathbf{F}_q$. Using this, the extremal property is straightfowardly extended to the case of some more general invariant polynomials. Duursma proved that all extremal Type IV codes satisfied the Riemann hypothesis ([7]). Thus, as far as the existing codes are concerned, we may expect that the Riemann hypothesis reflects one of the abilities of the code, the extremal property.

In [2], the author extended the consideration to the case of the formal weight enumerators. A formal weight enumerator $W(x,y)$ resembles the weight enumerator of a Type II code, but is distinguished from it by the property $W^{\sigma_2}(x,y) = -W(x,y)$ (see [2, Definition 1.4]). The zeta polynomial $P(T)$ of $W(x,y)$ satisfies $P(T) = -P(1/2T)2^gT^{2g}$ $(g = n/2+1-d)$ and we can formulate the Riemann hypothesis in the same way as in Definition 1.2, setting $q = 2$. In [2, Section 3], we observed that the extremal property might yield the Riemann hypothesis also in the case of the formal weight enumerators.

The purpose of the present article is to extend the consideration to all the polynomials which are invariant by the MacWilliams transform σ_q. Such polynomials form an invariant polynomial ring

$$\mathbf{C}[x,y]^{G_q} = \mathbf{C}[x+(\sqrt{q}-1)y, y(x-y)] \tag{1.5}$$

where $G_q = \langle \sigma_q \rangle$ (see MacWilliams-Sloane [9, p.605, Theorem 5]). As a problem of invariant polynomials, we can remove the structure of linear codes and allow q to be any positive integer such that $q \geq 2$. We try to find as many polynomials as possible in $\mathbf{C}[x,y]^{G_q}$ which satisfy the Riemann hypothesis. The results imply that the Riemann hypothesis is not always relevant to the extremal property in the ring $\mathbf{C}[x,y]^{G_q}$. The first result is the following:

Theorem 1.4 *For any $q \geq 2$ and any n, d such that $2 \leq d \leq \frac{n+1}{2}$, there exists a σ_q-invariant polynomial of the form (1.1) which satisfies the Riemann hypothesis.*

Note that the restriction $2 \leq d$ comes from the original Duursma theory. We also note that the number d in (1.1) must satisfy $d \leq \frac{n}{2}+1$ in $\mathbf{C}[x,y]^{G_q}$. In cases where equality holds, the polynomial becomes MDS and the zeta polynomial is a constant (see Section 3). Thus by the condition $2 \leq d \leq \frac{n+1}{2}$, almost all possible pairs of n and d are covered and it shows that polynomials satisfying the Riemann hypothesis are widely and abundantly distributed in $\mathbf{C}[x,y]^{G_q}$.

The notion of extremal polynomial is defined only in terms of n and d, but Theorem 1.4 implies that, at least in the ring $\mathbf{C}[x,y]^{G_q}$, the condition for the Riemann hypothesis is not determined by n and d only. Thus Theorem 1.4 shows us another aspect of the zeta functions for invariant polynomials.

Theorem 1.4 is proved by explicit construction of the invariant polynomials with the desired property. This is done by using the weight enumerators of codes which are not self-dual. If C is not self-dual, its weight enumarator $W_C(x,y)$ does not satisfy $W_C^{\sigma_q}(x,y) = W_C(x,y)$, but combining $W_C(x,y)$ and $W_{C^\perp}(x,y)$, we can easily get an invariant expression $\tilde{W}_C(x,y)$ and its zeta polynomial $\tilde{P}_C(T)$ (see Section 2). Theorem 1.4 is the result of the case where C is an MDS code (see Section 3).

Such a way of constructing invariant polynomials can be applied to any linear code which is not self-dual and leads to further exploration. The rest of the paper is devoted to the analysis of two other special classes of codes, the general Hamming codes and the Golay codes (not self-dual). These codes, along with certain MDS codes form an important class of good codes, the perfect codes (see Pless [11, p.21]):

Definition 1.5 *A code $C \subset \mathbf{F}_q{}^n$ of minimum distance d is called perfect if all the vectors in $\mathbf{F}_q{}^n$ are contained in a ball of radius $[(d-1)/2]$ about the codewords, where $[x]$ means the largest integer not greater than x.*

The nontrivial linear perfect codes are completely determined ([11, Section 2.2] or [9, Section 6.10]):

(i) The general Hamming $[(q^r-1)/(q-1)=n, n-r, 3]$ codes over $\mathbf{F}_q$,

(ii) The binary $[23,12,7]$ and the ternary $[11,6,5]$ Golay codes.

We also have trivial perfect codes: the whole space and a binary repetition code of odd length. The latter has the parameter $[n,1,n]$, being MDS and dealt with in Theorem 1.4. As to the general Hamming codes, they become MDS when $r=2$, so it follows that this case is also treated in Theorem 1.4.

We can find again infinitely many polynomials in $\mathbf{C}[x,y]^{G_q}$ satisfying the Riemann hypothesis by constructing $\tilde{W}_C(x,y)$ from the above class of codes:

Theorem 1.6 *Let $C=\mathrm{Ham}(r,q)$ be the Hamming $[(q^r-1)/(q-1)=n, n-r, 3]$ code over $\mathbf{F}_q$. If $r\geq 3$ and $q\geq 4$, then the invariant polynomial $\tilde{W}_C(x,y)$ in $\mathbf{C}[x,y]^{G_q}$ satisfies the Riemann hypothesis.*

To prove Theorem 1.6, we deduce a certain function theoretical result concerning the distribution of the zeros of a self-reciprocal polynomial:

Theorem 1.7 *If $f(T)=a_0+a_1T+\cdots+a_kT^k+a_kT^{m-k}+a_{k-1}T^{m-k+1}+\cdots+a_0T^m$ $(m>2k)$ satisfies $a_0>a_1>\cdots>a_k>0$, then all the roots of $f(T)$ lie on the unit circle.*

This is, so to speak, a self-reciprocal analogue of the famous Eneström-Kakeya theorem (see Theorem 5.1). Because of the technical difficulties, Theorem 1.6 remains unproved when $q=2,3$ and $r\geq 3$, but numerical experiments imply that the Riemann hypothesis seems to be true in these cases.

For the Golay codes, we have the following:

Theorem 1.8 *Let C be the binary $[23,12,7]$ or the ternary $[11,6,5]$ Golay code. Then the invariant polynomial $\tilde{W}_C(x,y)$ satisfies the Riemann hypothesis.*

Thus except for the binary and ternary general Hamming codes, we can prove that the invariant polynomials $\tilde{W}_C(x,y)$ from the perfect codes satisfy the Riemann hypothesis.

The rest of the article is organized as follows. In Section 2, we construct an invariant polynomial $\tilde{W}_C(x,y)$ from the weight enumerator of a code C (which is not always self-dual) and give an explicit form of its zeta polynomial $\tilde{P}_C(T)$. In Section 3, we apply the results in Section 2 to the MDS code and prove Theorem 1.4. In Section 4, we determine the zeta polynomial $\tilde{P}_C(T)$ when $C=\mathrm{Ham}(r,q)$, the general Hamming code when $r\geq 3$ and $q\geq 2$. Section 5 is devoted to an analogue of the Eneström-Kakeya theorem. Here we use several results of the classical function theory. Using it, we prove the Riemann hypothesis for $\tilde{W}_{\mathrm{Ham}(r,q)}(x,y)$ $(r\geq 3,\ q\geq 4)$ in Section 6. In Section 7, we consider the case of the Golay codes, and prove Theorem 1.8 by a different method to Theorem 1.6.

We have been interested in the extremal property of the weight enumerators when considering the Riemann hypothesis in the context of existing self-dual codes or a little larger class of invariant polynomials which have some connections to the coding theory, that is, the formal weight enumerators. But the results in this article show that it is not always the extremal property that yields the Riemann hypothesis in the "largest" ring $\mathbf{C}[x,y]^{G_q}$. We can observe rather pathological phenomena there. We are now in a position to seek some new structures which are larger than existing codes (but smaller than $\mathbf{C}[x,y]^{G_q}$), in which the Riemann hypothesis indicates some distinguished properties of invariant polynomials.

Acknowledgment. The author would like to express his sincere gratitude to Professor Leo Murata for an abundance of valuable advice and discussion.

2 Invariant polynomials and their zeta functions from arbitrary linear codes

Let C be a linear $[n,k,d]$ code over $\mathbf{F}_q$ and $W_C(x,y)$ be its Hamming weight enumerator. Suppose the dual code $C^\perp$ has the parameter $[n, n-k, d^\perp]$ and we assume $d, d^\perp \geq 2$. Combining $W_C(x,y)$ and the dual weight enumerator $W_{C^\perp}(x,y)$, we can easily obtain an invariant expression $\tilde{W}_C(x,y)$:

Proposition 2.1 *Let*

$$\tilde{W}_C(x,y) := \frac{1}{1+q^{k-n/2}}\{W_C(x,y) + q^{k-n/2}W_{C^\perp}(x,y)\}. \tag{2.1}$$

Then we have $\tilde{W}_C^{\sigma_q}(x,y) = \tilde{W}_C(x,y)$, *i.e.* $\tilde{W}_C(x,y) \in \mathbf{C}[x,y]^{G_q}$.

Proof. The proof is evident from the MacWilliams identity

$$W_C^{\sigma_q}(x,y) = q^{k-n/2}W_{C^\perp}(x,y) \quad \text{or} \quad W_{C^\perp}^{\sigma_q}(x,y) = q^{n/2-k}W_C(x,y)$$

(see [9, p.146, Theorem 13]). ∎

Now we deduce the explicit form of the zeta polynomial $\tilde{P}_C(T)$ of $\tilde{W}_C(x,y)$. Let $P_C(T)$ and $P_{C^\perp}(T)$ be the zeta polynomials of $W_C(x,y)$ and $W_{C^\perp}(x,y)$, respectively. Our goal in this section is to prove the following:

Theorem 2.2 *The zeta polynomial* $\tilde{P}_C(T)$ *of* $\tilde{W}_C(x,y)$ *is given by*

$$\tilde{P}_C(T) = \frac{T^{\max(0,d-d^\perp)}}{1+q^{k-n/2}}\left\{P_C(T) + q^{n/2+1-d}P_C\left(\frac{1}{qT}\right)T^{n+2-2d}\right\}. \tag{2.2}$$

It satisfies $\deg \tilde{P}_C = 2\tilde{g}$ *and the functional equation*

$$\tilde{P}_C(T) = \tilde{P}_C\left(\frac{1}{qT}\right)q^{\tilde{g}}T^{2\tilde{g}} \tag{2.3}$$

where $\tilde{g} := n/2 - 1 - \min(d, d^\perp)$.

Proof. By Definition 1.1, We have

$$\frac{P_C(T)}{(1-T)(1-qT)}(y(1-T)+xT)^n = \cdots + \frac{W_C(x,y)-x^n}{q-1}T^{n-d} + \cdots \tag{2.4}$$

and

$$\frac{P_{C^\perp}(T)}{(1-T)(1-qT)}(y(1-T)+xT)^n = \cdots + \frac{W_{C^\perp}(x,y)-x^n}{q-1}T^{n-d^\perp} + \cdots. \tag{2.5}$$

We suppose $d \le d^\perp$. Then (2.5) multiplied by $q^{k-n/2}T^{d^\perp-d}$ becomes

$$\frac{q^{k-n/2}P_{C^\perp}(T)T^{d^\perp-d}}{(1-T)(1-qT)}(y(1-T)+xT)^n = \cdots + \frac{q^{k-n/2}(W_{C^\perp}(x,y)-x^n)}{q-1}T^{n-d} + \cdots. \tag{2.6}$$

We add (2.4) and (2.6), then divide it by $1+q^{k-n/2}$. It gives

$$\frac{\{P_C(T)+q^{k-n/2}P_{C^\perp}(T)T^{d^\perp-d}\}/(1+q^{k-n/2})}{(1-T)(1-qT)}(y(1-T)+xT)^n = \cdots + \frac{\tilde{W}_C(x,y)-x^n}{q-1}T^{n-d} + \cdots.$$

Thus we have

$$\tilde{P}_C(T) = \frac{1}{1+q^{k-n/2}}\left\{P_C(T)+q^{k-n/2}P_{C^\perp}(T)T^{d^\perp-d}\right\} \tag{2.7}$$

by the existence and uniqueness of the zeta polynomial. The polynomial $P_{C^\perp}(T)$ can be substituted by

$$P_{C^\perp}(T) = P_C\left(\frac{1}{qT}\right)q^gT^{g+g^\perp}$$

where

$$\begin{aligned} g &= n+1-k-d, \qquad (2.8)\\ g^\perp &= k+1-d^\perp. \qquad (2.9)\end{aligned}$$

These formulas come from the original Duursma theory (see Duursma [5, p.59]). Hence we have

$$\tilde{P}_C(T) = \frac{1}{1+q^{k-n/2}}\left\{P_C(T)+q^{n/2+1-d}P_C\left(\frac{1}{qT}\right)T^{n+2-2d}\right\}. \tag{2.10}$$

When $d \ge d^\perp$, similarly we have

$$\tilde{P}_C(T) = \frac{T^{d-d^\perp}}{1+q^{k-n/2}}\left\{P_C(T)+q^{n/2+1-d}P_C\left(\frac{1}{qT}\right)T^{n+2-2d}\right\}. \tag{2.11}$$

These two formulas give (2.2). The functional equation (2.3) is obtained in a similar manner to that of Duursma [6, p.119]. As to $\deg \tilde{P}_C$, first we note that

$$\deg P_C = \deg P_{C^\perp} = g + g^\perp = n+2-d-d^\perp \tag{2.12}$$

(see [5, p.59]). By (2.7), we have $\deg \tilde{P}_C = n+2-2d = 2\tilde{g}$ when $d \le d^\perp$. The case $d \ge d^\perp$ is similar. ▮

Remark. When $C^\perp = C$, we can easily verify that $\tilde{P}_C(T) = P_C(T)$. Thus we have extended Duursma's theory in such a way that the zeta functions for codes which are not self-dual have the functional equation.

3 The MDS codes

We consider the case where C is an MDS code in the construction of $\tilde{W}_C(x,y)$ in Section 2 and prove Theorem 1.4. An $[n,k,d]$ code C is called an MDS (maximal distance separable) code if $d=n-k+1$ is satisfied, i.e., the equality holds in the Singleton bound $d \le n-k+1$. If C is MDS, then so is $C^\perp$ and it has the parameter $[n, n-k, n+2-d]$. The weight enumerator $W_C(x,y)$ of an MDS code C is determined only by n, d and q. It can be explicitly given in terms of binomial coefficients:

Theorem 3.1 *Let* $W_C(x,y)=\sum_{i=0}^n A_i x^{n-i}y^i$ *be the weight enumerator of an* $[n,k,d=n-k+1]$ *MDS code* C*. Then we have*

$$A_i = \binom{n}{i}\sum_{j=0}^{i-d}(-1)^j\binom{i}{j}(q^{i-d+1-j}-1). \quad (i \ge d)$$

Proof. MacWilliams-Sloane [9, p.320, Theorem 6]. ▮

We allow A_i to be negative and q be arbitrary integer greater than one. Even in the case $W_C(x,y)$ does not represent the weight distribution of an actual code, we are interested in the polynomial itself and often call it an "MDS polynomial". From now on we assume $d, d^\perp \ge 2$. What is crucial for our discussion is the following:

Theorem 3.2 *Let* C *be MDS. Then we have* $P_C(T)=1$.

Proof. See Duusrma [5, Proposition 1]. In cases where q is not a prime power, it is straightforward. ▮

Now we determine the range of d and n. Both C and $C^\perp$ are MDS, so we can assume $d \le d^\perp$ without loss of generality. Since $d^\perp = n+2-d$, $d \le d^\perp$ is equivalent to

$$d \le \frac{n}{2}+1. \tag{3.1}$$

If equality holds in (3.1), then $\tilde{g}=0$ and $\tilde{P}_C(T)$ is a constant ($\tilde{W}_C(x,y)$ is an MDS polynomial in the ring $\mathbf{C}[x,y]^{G_q}$ in this case. It can happen when n is even). We exclude this case and have $d \le (n+1)/2$. Duursma's theory requires $d, d^\perp \ge 2$, therefore d and n can assume the values with

$$2 \le d \le \frac{n+1}{2}. \tag{3.2}$$

Now let C be an (actual or virtual) MDS code. Then we have $P_C(T)=P_{C^\perp}(T)=1$ by Theorem 3.2. The zeta polynomial $\tilde{P}_C(T)$ of the invariant polynomial $\tilde{W}_C(x,y)$ is given by Theorem 2.2 as

$$\tilde{P}_C(T) = \frac{1}{1+q^{k-n/2}}(1+q^{n/2+1-d}T^{n+2-2d}). \tag{3.3}$$

We can easily see that all the roots of (3.3) lie on the circle $|T|=1/\sqrt{q}$. From Theorem 3.1 and (3.2), $\tilde{W}_C(x,y)$ is of the form $x^n + A_d x^{n-d}y^d + \cdots$ and $A_d \ne 0$. This completes the proof of Theorem 1.4.

4 The general Hamming codes

For $r \geq 2$ and a prime power q, the general Hamming $[(q^r-1)/(q-1)=n, n-r, 3]$ code $\mathrm{Ham}(r,q)$ over $\mathbf{F}_q$ is the dual code of an $[n, r, q^{r-1}]$ simplex code over $\mathbf{F}_q$ (see Pless et al. [12, p.316]). Therefore we have

$$\begin{aligned} W_{\mathrm{Ham}(r,q)^\perp}(x,y) &= x^n + (q-1)nx^{\frac{n-1}{q}}y^{\frac{(q-1)n+1}{q}} \\ &= x^n + (q^r-1)x^{n-q^{r-1}}y^{q^{r-1}}. \end{aligned} \tag{4.1}$$

In this section we assume $r \geq 3$, allow q to be any integer with $q \geq 2$ and determine explicitly the zeta polynomial $\tilde{P}_{r,q}(T) := \tilde{P}_{\mathrm{Ham}(r,q)}(T)$ of the invariant polynomial $\tilde{W}_{\mathrm{Ham}(r,q)}(x,y) \in \mathbf{C}[x,y]^{G_q}$ constructed in the manner of Section 2. For our purpose, it is easier to handle with $W_{\mathrm{Ham}(r,q)^\perp}(x,y)$ than $W_{\mathrm{Ham}(r,q)}(x,y)$, so we fix the notation as follows:

$$\begin{aligned} &C = \mathrm{Ham}(r,q)^\perp, \quad C^\perp = \mathrm{Ham}(r,q), \\ &n = \frac{q^r-1}{q-1} \qquad \text{(the length of } C \text{ and } C^\perp\text{)}, \\ &d = q^{r-1} \qquad \text{(the minimum distance of } \mathrm{Ham}(r,q)^\perp\text{)}. \end{aligned}$$

First we deduce the zeta polynomial $P_C(T) = P_{\mathrm{Ham}(r,q)^\perp}(T)$. We use the notion of the normalized weight enumerator (see Duursma [5, Definition 2]):

Definition 4.1 *For a weight enumerator $A(x,y)$ of the form (1.1), the normalized weight enumerator $a(t)$ is defined by*

$$a(t) = \frac{1}{q-1}\sum_{i=d}^{n} A_i \Big/ \binom{n}{i} t^{i-d}.$$

The following theorem gives the relation between $A(x,y)$ and its zeta polynomial $P(T)$:

Theorem 4.2 (Duursma) *The weight enumerator $A(x,y)$, its zeta polynomial $P(T)$ and the normalized weight enumerator $a(t)$ are related by*

$$\frac{P(T)}{(1-T)(1-qT)}(1-T)^{d+1} \equiv a\left(\frac{T}{1-T}\right) \pmod{T^{n-d+1}}.$$

Proof. See [5, Theorem 2]. ▮

For our code $C = \mathrm{Ham}(r,q)^\perp$, the normalized weight enumerator $a(t)$ is quite simple:

Lemma 4.3 *Let $a_{r,q}(t)$ be the normalized weight enumerator of* $\mathrm{Ham}(r,q)^\perp$. *Then*

$$a_{r,q}(t) = n \Big/ \binom{n}{q^{r-1}},$$

i.e., $a_{r,q}(t)$ is a constant.

The proof is easy from (4.1). Using this lemma and Theorem 4.2, we can deduce the explicit form of $P_C(T)$:

Proposition 4.4 *For $r \geq 3$ and $q \geq 2$, the zeta polynomial $P_C(T) = P_{\mathrm{Ham}(r,q)^\perp}(T)$ is given by*

$$P_C(T) = N_{r,q}\left[1 + \sum_{j=1}^{n-d-1}\left\{\binom{j+d-1}{d-1} - q\binom{j+d-2}{d-1}\right\}T^j\right], \tag{4.2}$$

where $n/\binom{n}{q^{r-1}}$.

Proof. Lemma 4.3 and Theorem 4.2 gives

$$\begin{aligned} P_C(T) &\equiv a\left(\frac{T}{1-T}\right)\frac{(1-T)(1-qT)}{(1-T)^{d+1}} \pmod{T^{n-d+1}} \\ &\equiv N_{r,q}\frac{1-qT}{(1-T)^d} \pmod{T^{n-d+1}}. \end{aligned} \tag{4.3}$$

We have

$$\deg P_C = n + 2 - d - 3 = n - d - 1 < n - d + 1$$

(see (2.12)), so $P_C(T)$ coincides with the power series expansion of $N_{r,q}(1-qT)/(1-T)^d$ up to the term of T^{n-d-1}. By the expansion $(1-T)^{-d} = \sum_{j=0}^{\infty}\binom{j+d-1}{d-1}T^j$, we have

$$\frac{1-qT}{(1-T)^d} = 1 + \sum_{j=1}^{\infty}\left\{\binom{j+d-1}{d-1} - q\binom{j+d-2}{d-1}\right\}T^j. \tag{4.4}$$

This formula gives the desired result. ▮

Remark. In the formula (4.4), $\binom{j+d-1}{d-1} - q\binom{j+d-2}{d-1} = 0$ holds if and only if $j = n - d$. Thus the term of T^{n-d} really vanishes in (4.4).

The main theorem in this section is the following:

Theorem 4.5 *For $r \geq 3$ and $q \geq 2$, the zeta polynomial $\tilde{P}_{r,q}(T) := \tilde{P}_{\mathrm{Ham}(r,q)}(T)$ is given by*

$$\tilde{P}_{r,q}(T) = \frac{N_{r,q}}{1 + q^{r-n/2}}(F_1(T) - qF_2(T)),$$

where

$$\begin{aligned} F_1(T) &= \sum_{i=0}^{n-d-1}\binom{n-i-2}{d-1}q^{i+2-n/2}T^i + \sum_{i=d-3}^{n-4}\binom{i+2}{d-1}T^i, \\ F_2(T) &= \sum_{i=0}^{n-d-2}\binom{n-i-3}{d-1}q^{i+2-n/2}T^i + \sum_{i=d-2}^{n-4}\binom{i+1}{d-1}T^i. \end{aligned}$$

Remark. If $r = 2$, both $\mathrm{Ham}(r,q)$ and $\mathrm{Ham}(r,q)^\perp$ are MDS codes and are treated in Section 3.

Proof. Since $d = q^{r-1} \geq 3$ if $r \geq 3$ and $q \geq 2$, we have from Theorem 2.2,

$$\tilde{P}_{r,q}(T) = \frac{T^{d-3}}{1 + q^{r-n/2}}\left\{P_C(T) + q^{n/2+1-d}P_C\left(\frac{1}{qT}\right)T^{n+2-2d}\right\}. \tag{4.5}$$

The remaining task is to describe each term in (4.5) explicitly. We have from Proposition 4.4,

$$\begin{aligned}\frac{T^{d-3}}{1+q^{r-n/2}}P_C(T) &= \frac{N_{r,q}}{1+q^{r-n/2}}\left[T^{d-3}+\sum_{j=1}^{n-d-1}\left\{\binom{j+d-1}{d-1}-q\binom{j+d-2}{d-1}\right\}T^{d+j-3}\right]\\ &= \frac{N_{r,q}}{1+q^{r-n/2}}\left[T^{d-3}+\sum_{i=d-2}^{n-4}\left\{\binom{i+2}{d-1}-q\binom{i+1}{d-1}\right\}T^{i}\right] \qquad (4.6)\end{aligned}$$

by putting $d+j-3=i$. Next we have from Proposition 4.4 again that

$$\begin{aligned}&\frac{T^{d-3}}{1+q^{r-n/2}}\cdot q^{n/2+1-d}P_C\left(\frac{1}{qT}\right)T^{n+2-2d}\\ &= \frac{N_{r,q}\,q^{n/2+1-d}}{1+q^{r-n/2}}\left[1+\sum_{j=1}^{n-d-1}\left\{\binom{j+d-1}{d-1}-q\binom{j+d-2}{d-1}\right\}q^{-j}T^{-j}\right]T^{n-d-1}\\ &= \frac{N_{r,q}}{1+q^{r-n/2}}\left[q^{n/2+1-d}T^{n-d-1}\right.\\ &\quad\left.+\sum_{j=1}^{n-d-1}\left\{\binom{j+d-1}{d-1}-q\binom{j+d-2}{d-1}\right\}q^{n/2+1-d-j}T^{n-d-j-1}\right]. \qquad (4.7)\end{aligned}$$

By substitution $n-d-j-1=i$, (4.7) equals

$$\frac{N_{r,q}}{1+q^{r-n/2}}\left[\sum_{i=0}^{n-d-2}\left\{\binom{n-i-2}{d-1}-q\binom{n-i-3}{d-1}\right\}q^{i+2-n/2}T^{i}+q^{n/2+1-d}T^{n-d-1}\right]. \qquad (4.8)$$

The formulas (4.5), (4.6) and (4.8) give

$$\begin{aligned}\tilde{P}_{r,q}(T) &= \frac{N_{r,q}}{1+q^{r-n/2}}\left[\sum_{i=0}^{n-d-2}\left\{\binom{n-i-2}{d-1}-q\binom{n-i-3}{d-1}\right\}q^{i+2-n/2}T^{i}\right.\\ &+ \left. q^{n/2+1-d}T^{n-d-1}+T^{d-3}+\sum_{i=d-2}^{n-4}\left\{\binom{i+2}{d-1}-q\binom{i+1}{d-1}\right\}T^{i}\right]. \qquad (4.9)\end{aligned}$$

We make $F_1(T)$ by gathering positive terms in (4.9) and $F_2(T)$ from negative ones. ∎

Theorem 1.6 claims that all the roots of $\tilde{P}_{r,q}(T)$ above lie on the circle $|T|=1/\sqrt{q}$ if $q\geq 4$. This is proved in several steps. We consider "normalized" zeta polynomial $\tilde{P}_{r,q}(T/\sqrt{q})$. Then the Riemann hypothesis is equivalent to the fact that all the roots of $\tilde{P}_{r,q}(T/\sqrt{q})$ lie on the unit circle. On the other hand, $\tilde{P}_{r,q}(T/\sqrt{q})$ is self-reciprocal, which is the result of the functional equation (1.3) ($\sum_{i=0}^{\nu}a_iT^i$ is called self-reciprocal if $a_i=a_{\nu-i}$ for all i). Moreover, if $q\geq 4$, $\tilde{P}_{r,q}(T/\sqrt{q})$ turns out to be of the form

$$\tilde{P}_{r,q}(T/\sqrt{q})=a_0+a_1T+\cdots+a_kT^k+a_kT^{m-k}+a_{k-1}T^{m-k+1}+\cdots+a_0T^m$$

with $m > 2k$ and $a_0 > a_1 > \cdots > a_k > 0$. We can prove that all the roots of a self-reciprocal polynomial of this form lie on the unit circle using several results of classical function theory (an analogue of the Eneström-Kakeya theorem, see Theorem 5.1). We state the proof in the next two sections.

Remark. We can also prove directly that $F_1(T/\sqrt{q})$, $F_2(T/\sqrt{q})$ and $\tilde{P}_{r,q}(T/\sqrt{q})$ are self-reciprocal, using the expressions in Theorem 4.5.

5 An analogue of the Eneström-Kakeya theorem

In this section, we prove Theorem 1.7. This is a self-reciprocal analogue of the following theorem and our proof of Theorem 1.7 is based on it:

Theorem 5.1 (Eneström-Kakeya) *Let $f(T) = a_0 + a_1 T + \cdots + a_k T^k$ satisfy $a_0 > a_1 > \cdots > a_k > 0$. Then $f(T)$ has no roots in $|T| \le 1$.*

Proof. Marden [10, p.151, Exercise 4]. ▮

Now, suppose a self-reciprocal polynomial

$$f(T) = a_0 + a_1 T + \cdots + a_k T^k + a_k T^{m-k} + a_{k-1} T^{m-k+1} + \cdots + a_0 T^m \quad (m > 2k) \tag{5.1}$$

satisfies $a_0 > a_1 > \cdots > a_k > 0$. We write $f(T)$ as a sum of two polynomials $P(T)$ and $Q(T)$:

$$\begin{aligned} P(T) &:= a_k T^{m-k} + a_{k-1} T^{m-k+1} + \cdots + a_0 T^m, \\ Q(T) &:= a_0 + a_1 T + \cdots + a_k T^k, \end{aligned} \tag{5.2}$$

so $f(T) = P(T) + Q(T)$. Then, by the assumption $a_0 > a_1 > \cdots > a_k > 0$, we can see from Theorem 5.1 that $Q(T)$ has no roots in $|T| \le 1$. We apply Rouché's theorem to $f(T)$. For simplicity, we state it in a restricted form:

Theorem 5.2 *Let C be a circle in $\mathbf{C}$, D be the inside of C. Suppose functions $P(T)$ and $Q(T)$ are holomorphic in $C \cup D$ and $|P(T)| < |Q(T)|$ on C. Then $Q(T)$ and $P(T) + Q(T)$ have the same number of zeros in D.*

Proof. Ahlfors [1, p.153, Corollary]. See also Lehmer [8, Lemma 3]. ▮

For our polynomials $P(T)$ and $Q(T)$, we can prove the following:

Theorem 5.3 *We have $|P(T)| < |Q(T)|$ on $|T| = r$ for any r with $0 < r < 1$.*

By this theorem, we can see that $Q(T)$ and $f(T) = P(T) + Q(T)$ have the same number of roots in $|T| < r$. By Theorem 5.1 again, $f(T)$ has no roots in $|T| < r$. Since r is arbitrary in $0 < r < 1$, we can verify that $f(T)$ has no roots in $|T| < 1$. Now recall that $f(T)$ is self-reciprocal. We have

$$T^m f\left(\frac{1}{T}\right) = f(T).$$

From this formula, we see that there is a one-to-one correspondence between a root in $|T| < 1$ and that in $|T| > 1$. We can conclude that $f(T)$ has no roots also in $|T| > 1$, and all the roots of $f(T)$ lie on $|T| = 1$. Hence we get Theorem 1.7.

Proof of Theorem 5.3.

First we need the following:

Lemma 5.4 (Lagrange's identity) *For any $A_i, B_i \in \mathbf{C}$, we have*

$$|\sum_{i=0}^{k} A_i B_i|^2 = \sum_{i=0}^{k} |A_i|^2 \sum_{i=0}^{k} |B_i|^2 - \sum_{0 \le i < j \le k} |A_i \overline{B_j} - A_j \overline{B_i}|^2.$$

Proof. Ahlfors [1, p.9, Exercise 5]. ▮

Using this, we can prove the following:

Lemma 5.5 *For $P(T)$ and $Q(T)$ in (5.2), we have*

$$|P(T)| = |Q(T)|$$

on $|T| = 1$.

Proof. By letting $A_i = a_i$ and $B_i = T^i$ in Lemma 5.4, we get

$$|Q(T)|^2 = (k+1)(a_0^2 + \cdots + a_k^2) - \sum_{0 \le i < j \le k} |a_i - a_j T^{j-i}|^2 \tag{5.3}$$

since $|T| = 1$. As to $P(T)$, noting that $|P(T)| = |a_k + a_{k-1}T + \cdots + a_0 T^k|$ on $|T| = 1$, we have

$$|P(T)|^2 = (k+1)(a_0^2 + \cdots + a_k^2) - \sum_{0 \le i < j \le k} |a_{k-i} - a_{k-j} T^{j-i}|^2 \tag{5.4}$$

by letting $A_i = a_{k-i}$ and $B_i = T^i$ in Lemma 5.4. By change of suffices in the sum in (5.4), we have

$$\sum_{0 \le i < j \le k} |a_{k-i} - a_{k-j} T^{j-i}|^2 = \sum_{0 \le j' < i' \le k} |a_{i'} - a_{j'} T^{i'-j'}|^2 = \sum_{0 \le i < j \le k} |a_j - a_i T^{j-i}|^2. \tag{5.5}$$

We compare the term for (i, j) in (5.3) and (5.5):

$$\begin{aligned} |a_i - a_j T^{j-i}|^2 - |a_j - a_i T^{j-i}|^2 &= (a_i - a_j T^{j-i})(a_i - a_j \overline{T}^{j-i}) - (a_j - a_i T^{j-i})(a_j - a_i \overline{T}^{j-i}) \\ &= 0 \end{aligned}$$

since $|T| = 1$. We see that the sums in the right hand sides in (5.3) and (5.4) are the same, and we obtain $|P(T)| = |Q(T)|$ on $|T| = 1$. ▮

The proof of Theorem 5.3 is completed by invoking the following well-known result:

Theorem 5.6 (The maximum principle) *Let $g(T)$ be holomorphic and nonconstant in a bounded (open) region $D \subset \mathbf{C}$ and continuous in $\overline{D}$ (the closure of D). Then $|g(T)|$ has its maximum M on $\overline{D} - D$ and we have*

$$|g(T)| < M$$

in D.

Proof. Ahlfors [1, p.134]. ▮

We apply Theorem 5.6 to $g(T) := P(T)/Q(T)$ and $D := \{T \in \mathbf{C} \ ; \ |T| < 1\}$. Clearly $g(T)$ is meromorphic and nonconstant. It has no pole in $\overline{D}$ by Theorem 5.1. Moreover, from Lemma 5.5, $|g(T)| = 1$ on the boundary of D. Therefore $|g(T)| < 1$ in D by Theorem 5.6 and we get Theorem 5.3.

6 Proof of Theorem 1.6

In this section, we prove Theorem 1.6. We have from Theorem 4.5,

$$\tilde{P}_{r,q}\left(\frac{T}{\sqrt{q}}\right) = \frac{N_{r,q}}{1+q^{r-n/2}}\left(F_1\left(\frac{T}{\sqrt{q}}\right) - qF_2\left(\frac{T}{\sqrt{q}}\right)\right)$$

where

$$F_1\left(\frac{T}{\sqrt{q}}\right) = \sum_{i=0}^{n-d-1}\binom{n-i-2}{d-1}q^{(i-n)/2+2}T^i + \sum_{i=d-3}^{n-4}\binom{i+2}{d-1}q^{-i/2}T^i, \tag{6.1}$$

$$F_2\left(\frac{T}{\sqrt{q}}\right) = \sum_{i=0}^{n-d-2}\binom{n-i-3}{d-1}q^{(i-n)/2+2}T^i + \sum_{i=d-2}^{n-4}\binom{i+1}{d-1}q^{-i/2}T^i. \tag{6.2}$$

Note that $n-d-1 < d-3$ if $r \geq 3$ and $q \geq 4$. So there is no term of the same degree from two summations in $F_1(T)$ of Theorem 4.5. Moreover, $\tilde{P}_{r,q}(T/\sqrt{q})$ is self-reciprocal. It follows from the functional equation (1.3), but we can verify it directly by showing $F_1(T/\sqrt{q})$ and $F_2(T/\sqrt{q})$ are self-reciprocal. Hence we can assume $\tilde{P}_{r,q}(T/\sqrt{q})$ is of the form (5.1). Let

$$\frac{1+q^{r-n/2}}{N_{r,q}}\tilde{P}_{r,q}(T/\sqrt{q}) = a_0 + a_1T + \cdots + a_{n-d-1}T^{n-d-1} + a_{n-d-1}T^{d-3} + \cdots + a_0T^{n-4}. \tag{6.3}$$

Lemma 6.1 *If $r \geq 3$ and $q \geq 4$, we have*

$$a_{n-d-2} > a_{n-d-1} > 0.$$

Proof. Recall $d = q^{r-1}$. Using the expressions (6.1) and (6.2), we have

$$a_{n-d-2} = q^{2-d/2}(q^{r-2}-1)$$

and

$$a_{n-d-1} = q^{(3-d)/2}.$$

Therefore, $a_{n-d-1} > 0$ and

$$a_{n-d-2} - a_{n-d-1} = q^{(3-d)/2}\{\sqrt{q}(q^{r-2}-1)-1\}.$$

The last expression is positive if $r \geq 3$ and $q \geq 4$. ▮

Lemma 6.2 *If $r \geq 3$ and $q \geq 4$, we have*

$$a_i > a_{i+1}$$

for $0 \leq i \leq n-d-3$.

Proof. Using the expressions (6.1) and (6.2), we have

$$\begin{aligned} a_i &= \binom{n-i-2}{d-1} q^{(i-n)/2+2} - \binom{n-i-3}{d-1} q^{(i-n)/2+3}, \\ a_{i+1} &= \binom{n-i-3}{d-1} q^{(i-n+5)/2} - \binom{n-i-4}{d-1} q^{(i-n+7)/2}. \end{aligned}$$

From these formulas, we have

$$\left\{ q^{(i-n)/2+2} \binom{n-i-4}{d-1} \right\}^{-1} (n-d-i-1)(n-d-i-2)(a_i - a_{i+1})$$

$$= (n-i-2)(n-i-3) - (n-i-3)(n-d-i-1)(q+\sqrt{q}) + (n-d-i-1)(n-d-i-2)q\sqrt{q}.$$

It suffices to show that the right hand side is positive. It is a quadratic function of the parameter i, so we denote it by $g(i) = ai^2 + bi + c$. We can show that $a, b, c > 0$ if $q \geq 4$. Indeed, first we have

$$a = q\sqrt{q} + 1 - (q + \sqrt{q}) = (\sqrt{q} - 1)(q - 1) > 0$$

if $q \geq 2$. As to b, recall $n = (q^r - 1)/(q - 1)$ and $d = q^{r-1}$. We have

$$\sqrt{q}(q-1)b = q^r(\sqrt{q} - 1)(q - 1) + q^{3/2}(3q^{3/2} - 4q - 5\sqrt{q} + 7) + \sqrt{q}(2\sqrt{q} - 3)$$

(such calculation can be easily done with the help of some expression manipulation program). As above, $q^r(\sqrt{q} - 1)(q - 1) > 0$ if $q \geq 2$ and $2\sqrt{q} - 3 > 0$ if $q \geq 3$. We can easily show $3q^{3/2} - 4q - 5\sqrt{q} + 7 > 0$ if $q \geq 4$ (show that $(3q^{3/2} - 4q - 5\sqrt{q} + 7)|_{q=4} > 0$ and $(3q^{3/2} - 4q - 5\sqrt{q} + 7)' > 0$ in $q \geq 4$). Therefore $b > 0$ if $q \geq 4$.

We can similarly show $c > 0$. Because

$$\begin{aligned} \sqrt{q}(q-1)^2 c &= q^r\{q(q^{3/2} - 2q - 2q^{1/2} + 4) + (q^{1/2} - 2)\} \\ &+ q^{5/2}(2q^{3/2} - 3q - 4q^{1/2} + 7) \\ &+ q^{1/2}(q^2 + 2q^{3/2} - 7q + 2), \end{aligned}$$

and we can show that $q^{3/2} - 2q - 2q^{1/2} + 4 \geq 0$ if $q \geq 4$, and that all other functions in the parentheses ( ) are positive in $q \geq 4$.

It follows that $g(i) > 0$ if $i \geq 0$ and $a_i - a_{i+1} > 0$. ∎

We can conclude from Lemmas 6.1 and 6.2 that

$$a_0 > a_1 > \cdots > a_{n-d-1} > 0 \tag{6.4}$$

for the coefficients in (6.3). The assumption of Theorem 1.7 is satisfied and the proof of Theorem 1.6 is completed.

Remark. (1) If we write $\tilde{W}_{\mathrm{Ham}(r,q)}(x, y)$ in the form (1.1), $n = (q^r - 1)/(q - 1)$ and $d = 3$. Thus we have found infinitely many invariant polynomials satisfying the Riemann hypothesis for a small d.

(2) When $q = 2, 3$, the coefficients of $\tilde{P}_{r,q}(T/\sqrt{q})$ does not satisfy (6.4) as the following examples show. So, in these cases, we cannot prove the Riemann hypothesis in a method described so far, but numerical experiments imply that it is very plausible that the Riemann hypothesis is true also for $q = 2, 3$.

Example 6.3 (i) Let $r = 3$, $q = 2$. Then

$$\tilde{W}_{\mathrm{Ham}(3,2)}(x,y) = x^7 + \frac{7}{1+\sqrt{2}}x^4y^3 + 7x^3y^4 + \frac{7}{1+\sqrt{2}}y^7,$$

$$\begin{aligned} F_1(T) - 2F_2(T) &= \frac{1}{\sqrt{2}} + (1+\sqrt{2})T + (2+\sqrt{2})T^2 + 2T^3, \\ F_1\left(\frac{T}{\sqrt{2}}\right) - 2F_2\left(\frac{T}{\sqrt{2}}\right) &= \frac{1}{\sqrt{2}} + \left(1+\frac{1}{\sqrt{2}}\right)T + \left(1+\frac{1}{\sqrt{2}}\right)T^2 + \frac{1}{\sqrt{2}}T^3 \\ &= \frac{1}{\sqrt{2}}(T+1)\left(T - \frac{-1+i}{\sqrt{2}}\right)\left(T - \frac{-1-i}{\sqrt{2}}\right). \end{aligned}$$

Hence $\tilde{W}_{\mathrm{Ham}(3,2)}(x,y)$ satisfies the Riemann hypothesis.

(ii) Let $r = 4$, $q = 2$. Then $\tilde{P}_{4,2}(T/\sqrt{q})$ is of degree 11. We normalize $\tilde{P}_{4,2}(T/\sqrt{q})$ with a suitable constant C as $C\tilde{P}_{4,2}(T/\sqrt{q}) = 1 + a_1T + \cdots$. Then we can approximate the coefficients as follows:

$$\begin{array}{ll} a_0 = 1 & a_3 \approx 1.028518954 \\ a_1 \approx 1.414213562 & a_4 \approx 0.606060606 \\ a_2 \approx 1.363636363 & a_5 \approx 0.317735799 \end{array}$$

and $a_6, \cdots, a_{11}$ are the same as above in the reverse order. We have $a_0 < a_1 > a_2 > a_3 > a_4 > a_5 > 0$, but according to the numerical experiment, $\tilde{W}_{\mathrm{Ham}(4,2)}(x,y)$ seems to satisfy the Riemann hypothesis.

(iii) Let $r = 5$, $q = 2$. Then $\tilde{P}_{5,2}(T/\sqrt{q})$ is of degree 27. Choose C as $C\tilde{P}_{5,2}(T/\sqrt{q}) = 1 + a_1T + \cdots$. Then the coefficients are approximated as

$$\begin{array}{lr} a_0 = 1 & a_7 \approx 0.2623468638 \\ a_1 \approx 1.414213562 & a_8 \approx 0.1391304348 \\ a_2 \approx 1.444444444 & a_9 \approx 0.0655867159 \\ a_3 \approx 1.257078722 & a_{10} \approx 0.0268497330 \\ a_4 \approx 0.977777778 & a_{11} \approx 0.0092051531 \\ a_5 \approx 0.691393297 & a_{12} \approx 0.0024887453 \\ a_6 \approx 0.446376812 & a_{13} \approx 0.0005216551 \end{array}$$

and $a_{14}, \cdots, a_{27}$ are the same as above in the reverse order. In this case we have $a_0 < a_1 < a_2 > a_3 > \cdots > a_{13} > 0$. The Riemann hypothesis seems to be true.

Example 6.4 Let $r = 3$, $q = 3$. Then $\tilde{P}_{3,3}(T/\sqrt{q})$ is of degree 9. Choose C as $C\tilde{P}_{3,3}(T/\sqrt{q}) = 1 + a_1T + \cdots$. Then $a_1 \approx 1.039230485$, $a_2 = 0.6$, $a_3 \approx 0.1732050808$, $a_4 = a_5 = 0$, and $a_6, \cdots, a_9$ are the same but in the reverse order. The Riemann hypothesis seems to be true. In many other $\mathrm{Ham}(r,3)$ with $r \geq 4$, we can observe that the coefficient of T in $\tilde{P}_{r,3}(T/\sqrt{q})$ is greater than the constant term.

7 The Golay codes

In this section we consider the case where $C = \mathcal{G}_{23}$, the binary $[23,12,7]$ Golay code or $C = \mathcal{G}_{11}$, the ternary $[11,6,5]$ Golay code. We have

$$\begin{aligned} W_{\mathcal{G}_{23}}(x,y) &= x^{23} + 253x^{16}y^7 + 506x^{15}y^8 + 1288x^{12}y^{11} + 1288x^{11}y^{12} + 506x^8y^{15} \\ &\quad +253x^7y^{16} + y^{23}, \qquad (7.1) \\ W_{\mathcal{G}_{11}}(x,y) &= x^{11} + 132x^6y^5 + 132x^5y^6 + 330x^3y^8 + 110x^2y^9 + 24y^{11} \qquad (7.2) \end{aligned}$$

(see [12, p.94]) or

$$\begin{aligned} W_{\mathcal{G}_{23}{}^\perp}(x,y) &= x^{23} + 506x^{15}y^8 + 1288x^{11}y^{12} + 253x^7y^{16}, \qquad (7.3) \\ W_{\mathcal{G}_{11}{}^\perp}(x,y) &= x^{11} + 132x^5y^6 + 110x^2y^9. \qquad (7.4) \end{aligned}$$

The case $C = \mathcal{G}_{11}$ is quite easy:

Proposition 7.1 *The zeta polynomial $\tilde{P}_{\mathcal{G}_{11}}(T)$ of the invariant polynomial $\tilde{W}_{\mathcal{G}_{11}}(x,y)$ is given by*

$$\tilde{P}_{\mathcal{G}_{11}}(T) = \frac{\sqrt{3}-1}{14}(\sqrt{3}T+1)(3T^2+3T+1).$$

All the roots of $\tilde{P}_{\mathcal{G}_{11}}(T)$ lie on the circle $|T| = 1/\sqrt{3}$.

Proof. The explicit form of $\tilde{P}_{\mathcal{G}_{11}}(T)$ can be obtained by computer calculation. The latter statement is obvious. ▮

Next we consider $C = \mathcal{G}_{23}$. By computer calculation we get the following:

Proposition 7.2 *Let $\tilde{P}_{\mathcal{G}_{23}}(T)$ be the zeta polynomial of the invariant polynomial $\tilde{W}_{\mathcal{G}_{23}}(x,y)$. Then*

$$\begin{aligned} \frac{25194}{2-\sqrt{2}}\tilde{P}_{\mathcal{G}_{23}}\left(\frac{T}{\sqrt{2}}\right) &= 13(1+T^{11}) + (13+39\sqrt{2})(T+T^{10}) \\ &+ (130+39\sqrt{2})(T^2+T^9) + (130+156\sqrt{2})(T^3+T^8) \\ &+ \frac{591+312\sqrt{2}}{2}(T^4+T^7) + \frac{591+459\sqrt{2}}{2}(T^5+T^6). \qquad (7.5) \end{aligned}$$

The polynomial $\tilde{P}_{\mathcal{G}_{23}}(T/\sqrt{2})$ does not satisfy the assumption of Theorem 1.7. We would like to verify the Riemann hypothesis for $\tilde{W}_{\mathcal{G}_{23}}(x,y)$ as theoretically as possible. Our method is influenced by that of Duursma [6, Section 5] and [7, Section 5].

Let $f(x)$ be a real polynomial of degree n. Then $f^*(T) = T^n f((T+T^{-1})/2)$ is a self-reciprocal polynomial of degree $2n$. If $T = e^{i\theta}$, then $(T+T^{-1})/2 = \cos\theta$, so the behavior of $f^*(T)$ on the unit circle can be captured by the behavior of $f(x)$ in the interval $[-1,1]$. We denote this mapping by ρ:

$$\rho : f \mapsto f^*. \qquad (7.6)$$

We would like to pull back $f(x)$ from a given self-reciprocal polynomial $f^*(T)$. It turns out that the inverse mapping ρ^{-1} always exists. To clarify this, we introduce two linear spaces of polynomials:

$$\begin{aligned} V_n &:= \{a_0 + a_1x + \cdots + a_nx^n \ ; \ a_j \in \mathbf{R}\}, \\ W_n &:= \{b_0 + b_1T + \cdots + b_nT^n + b_{n-1}T^{n+1} + \cdots b_0T^{2n} \ ; \ b_j \in \mathbf{R}\}. \end{aligned}$$

The operations in the vector spaces are the same as ordinary summation of polynomials and multiplication by real numbers.

Lemma 7.3 *The mapping $\rho : V_n \to W_n$ defined by (7.6) is a linear isomorphism.*

Proof. Clearly ρ is linear. For the later use, we describe the matrix A_ρ of ρ with respect to the bases

$$\begin{aligned} V_n &= \mathbf{R}[1, x, \cdots, x^n], \\ W_n &= \mathbf{R}[T^n, T^{n-1} + T^{n+1}, \cdots 1 + T^{2n}]. \end{aligned}$$

Because ρ maps $1, x, x^2, \cdots$ as

$$\begin{aligned} 1 &\mapsto T^n, \\ x &\mapsto \frac{\binom{1}{0}}{2}(T^{n-1} + T^{n+1}), \\ x^2 &\mapsto \frac{\binom{2}{0}}{2^2}(T^{n-2} + T^{n+2}) + \frac{\binom{2}{1}}{2^2}T^n, \\ x^3 &\mapsto \frac{\binom{3}{0}}{2^3}(T^{n-3} + T^{n+3}) + \frac{\binom{3}{1}}{2^3}(T^{n-1} + T^{n+1}), \\ x^4 &\mapsto \frac{\binom{4}{0}}{2^4}(T^{n-4} + T^{n+4}) + \frac{\binom{4}{1}}{2^4}(T^{n-2} + T^{n+2}) + \frac{\binom{4}{2}}{2^4}T^n, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots . \end{aligned}$$

we have for even n,

$$A_\rho = \begin{bmatrix} 1 & 0 & 2^{-2}\binom{2}{1} & 0 & 2^{-4}\binom{4}{2} & \cdots & 2^{-n}\binom{n}{n/2} \\ & 2^{-1}\binom{1}{0} & 0 & 2^{-3}\binom{3}{1} & 0 & \cdots & 0 \\ & & 2^{-2}\binom{2}{0} & 0 & 2^{-4}\binom{4}{1} & \cdots & 2^{-n}\binom{n}{n/2-1} \\ & & & 2^{-3}\binom{3}{0} & 0 & \cdots & 0 \\ & & & & 2^{-4}\binom{4}{0} & \cdots & 2^{-n}\binom{n}{n/2-2} \\ & & & & & \ddots & \vdots \\ & & & & & & 2^{-n}\binom{n}{0} \end{bmatrix},$$

where all the elements in the lower triangular part are zero. If n is odd, the $(n+1)$-th column is replaced by ${}^t[0, 2^{-n}\binom{n}{(n-1)/2}, 0, 2^{-n}\binom{n}{(n-1)/2-1}, \cdots, 2^{-n}\binom{n}{0}]$. By this expression, $\det A_\rho = 2^{-n(n+1)/2} \neq 0$, so A_ρ is regular. ▮

We sketch the proof that all the roots of $\tilde{P}_{\mathcal{G}_{23}}(T/\sqrt{2})$ lie on the unit circle. The calculation is done with the help of a computer. Let $F(T) = (25194/(2-\sqrt{2}))\tilde{P}_{\mathcal{G}_{23}}(T^2/\sqrt{2})$. Then $\deg F = 22$ and $F(T)$ is self-reciprocal. Construct A_ρ for $n = 11$ and map $F(T)$ by ρ^{-1} using ${A_\rho}^{-1}$. Then we have

$$\begin{aligned} (\rho^{-1}F)(x) &= 26624x^{11} + (-66560 + 19968\sqrt{2})x^9 \\ &+ (74880 - 39936\sqrt{2})x^7 + (-45760 + 29952\sqrt{2})x^5 \\ &+ (14324 - 9984\sqrt{2})x^3 + (-1754 + 1239\sqrt{2})x. \end{aligned}$$

We can also verify $(\rho^{-1}F)(-1) < 0$, $(\rho^{-1}F)(-0.8) > 0$, $(\rho^{-1}F)(-0.6) < 0$, $(\rho^{-1}F)(-0.4) > 0$, $(\rho^{-1}F)(-0.2) < 0$, $(\rho^{-1}F)(-0.1) > 0$. It follows that $(\rho^{-1}F)(x)$ has at least five roots in the interval $(-1, 0)$. It has the same number of roots in $(0, 1)$ since it is an odd function of x, and $(\rho^{-1}F)(0) = 0$. Thus all the roots of $(\rho^{-1}F)(x)$ are distinct and lie in $(-1, 1)$. Let $T = e^{i\theta}$. Then $x = \cos\theta$. While x moves from 1 to -1, T^2 goes once around the unit circle. Therefore $\tilde{P}_{\mathcal{G}_{23}}(T^2/\sqrt{2})$ assumes zero exactly 11 times on $|T| = 1$.

8 Appendix — an elementary proof of existence of $P(T)$

Existence and uniqueness of the zeta polynomial $P(T)$ for a linear code was first established in [4, Section 9], but a detailed proof is not given. Here we give an alternative, elementary proof, including the case $W(x,y) \in \mathbf{C}[x,y]$.

Suppose $W(x,y) \in \mathbf{C}[x,y]$ is a polynomial of the form (1.1). First note that

$$\begin{aligned} f(T) := & \frac{1}{(1-T)(1-qT)}(y(1-T)+xT)^n \\ &= (1+T+T^2+\cdots)(1+qT+q^2T^2+\cdots)((x-y)T+y)^n \\ &= (1+c_1T+c_2T^2+\cdots)\Big\{\sum_{j=0}^{n}\binom{n}{j}(x-y)^j y^{n-j}T^j\Big\} \end{aligned}$$

for some $c_j \in \mathbf{N}$. Expanding the last formula, we find for some integers b_{ij},

$$\begin{array}{lr} \text{the constant term} & = y^n, \\ \text{the coefficient of } T & = nxy^{n-1}+(c_1-n)y^n, \\ \cdots\cdots & \cdots\cdots\cdots \\ \text{the coefficient of } T^i & = b_{i0}x^iy^{n-i}+b_{i1}x^{i-1}y^{n-i+1}+\cdots+b_{ii}y^n, \\ \cdots\cdots & \cdots\cdots\cdots \\ \text{the coefficient of } T^{n-d} & = b_{n-d,0}x^{n-d}y^d+b_{n-d,1}x^{n-d-1}y^{d+1}+\cdots+b_{n-d,n-d}y^n. \end{array}$$

Let a_0, a_1, $\cdots$, $a_{n-d} \in \mathbf{C}$ and we form a function $F(T) := (a_0+a_1T+\cdots+a_{n-d}T^{n-d})f(T)$. Then the coefficient of T^{n-d} of $F(T)$ is

$$\begin{aligned} & a_{n-d}y^n \\ & +a_{n-d-1}\{nxy^{n-1}+(c_1-n)y^n\} \\ & \cdots\cdots\cdots \\ & +a_i\{b_{i0}x^iy^{n-i}+b_{i1}x^{i-1}y^{n-i+1}+\cdots+b_{ii}y^n\} \\ & \cdots\cdots\cdots \\ & +a_0\{b_{n-d,0}x^{n-d}y^d+b_{n-d,1}x^{n-d-1}y^{d+1}+\cdots+b_{n-d,n-d}y^n\}. \end{aligned} \tag{8.1}$$

On the other hand, since $(W(x,y)-x^n)/(q-1) = (A_dx^{n-d}y^d+\cdots+A_ny^n)/(q-1)$, we can determine a_0, a_1, $\cdots$, a_{n-d} so that (8.1) coincides with $(W(x,y)-x^n)/(q-1)$ (the system of linear equations for determining a_0, a_1, $\cdots$, a_{n-d} has a regular coefficient matrix). So we can always determine the zeta polynomial $P(T)$ from a given $W(x,y)$ uniquely as $P(T) = a_0+a_1T+\cdots+a_{n-d}T^{n-d}$. ▮

References

[1] Ahlfors, L. V. : Complex Analysis, 3rd Ed., McGrow-Hill, 1979.

[2] Chinen, K. : Zeta functions for formal weight enumerators and the extremal property, Proc. Japan Acad. **81** Ser. A. (2005), 168 - 173.

[3] Conway, J, H. and Sloane, N. J. A. : Sphere Packings, Lattices and Groups, 3rd Ed., Springer Verlag, 1999.

[4] Duursma, I. : Weight distribution of geometric Goppa codes, Trans. Amer. Math. Soc. **351**, No.9 (1999), 3609-3639.

[5] ________ : From weight enumerators to zeta functions, Discrete Appl. Math. **111** (2001), 55-73.

[6] ________ : A Riemann hypothesis analogue for self-dual codes, DIMACS series in Discrete Math. and Theoretical Computer Science **56** (2001), 115-124.

[7] ________ : Extremal weight enumerators and ultraspherical polynomials, Discrete Math. **268**, No.1-3 (2003), 103-127.

[8] Lehmer, D. H. : A machine method for solving polynomial equations, J. Assoc. Comput. Mach. **8** (1961), 151-162.

[9] MacWilliams, F. J. and Sloane, N. J. A. : The Theory of Error-Correcting Codes, North-Holland, 1977.

[10] Marden, M. : The Geometry of the Zeros of a Polynomial in a Complex Variable, Math. Surveys 3, Amer. Math. Soc., 1949.

[11] Pless, V. : Introduction to the Theory of Error-Correcting Codes, John Wiley & Sons, 1998 (Third Edition).

[12] Pless, V. and Huffman, W. (eds.) : Handbook of Coding Theory, I, II, Elsevier Science B. V., 1998.